IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

K. MIZRA, LLC Plaintiff, v. CISCO SYSTEMS, INC. Defendant,	Civil Action No. 6:20-CV-01031-ADA JURY TRIAL DEMANDED

DEFENDANT'S AMENDED ANSWER. AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS

Defendant Cisco Systems, Inc. ("Cisco") hereby files its Answer and Affirmative Defenses to K. Mizra, LLC ("K.Mizra")'s First Amended Complaint for Patent Infringement.

NATURE OF THE CASE

Complaint Paragraph 1:

1. This is an action for the infringement of two United States Patents: (1) U.S. Patent No. 8,234,705 (the " '705 patent") and (2) U.S. Patent No. 8,965,892 (the " '892 patent"), collectively referred to as "the Patents-in-Suit."

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegation that K.Mizra has clear title and standing to sue for infringement as the rightful owner of U.S. Patent Nos. 8,234,705 ("the '705 patent") and No. 8,965,892 ("the '892 patent") and therefore denies that allegation. Cisco admits that the '705 patent and '892 patent are respectively titled as alleged in Paragraph 1 of the Complaint and that together they are "the Patents-in-Suit."

Complaint Paragraph 2:

2. Defendant Cisco has been making, selling, using and offering for sale computer network security products such as the Cisco Identity Services Engine ("ISE"), Cisco Secure Network Server, and various other Cisco network equipment and software incorporating similar technology that infringe the '705 patent in violation of 35 U.S.C. § 271.

Response: Cisco admits that it makes, uses, imports, distributes, markets, sells and/or offers to sell products and/or services throughout the United States, including in this judicial district, but denies that any such products and/or services infringe any valid and enforceable claim of the Patents-in-Suit.

Complaint Paragraph 3:

3. Defendant Cisco has been making, selling, using and offering for sale email security products such as the Cisco Email Security software, appliances, and various other Cisco network equipment and software incorporating its email security protection technology that infringe the '892 patent in violation of 35 U.S.C. § 271.

Response: Cisco admits that it makes, uses, imports, distributes, markets, sells and/or offers to sell products and/or services throughout the United States, including in this judicial district, but denies that any such products and/or services infringe any valid and enforceable claim of the Patents- in-Suit.

Complaint Paragraph 4:

4. Plaintiff K.Mizra seeks appropriate damages and prejudgment and post judgment interest for Cisco's infringement of the Patents-in-Suit.

Response: Denied.

THE PARTIES

Complaint Paragraph 5:

5. Plaintiff K.Mizra is a Delaware corporation with its principal place of business at 2160 Century Park East #707, Los Angeles, CA 90067. K.Mizra is the assignee and owner of the Patents-in-Suit.

Response: Cisco admits, on information and belief, that K.Mizra is a limited liability company existing under the laws of Delaware with its principal place of business in Los Angeles, California.

Complaint Paragraph 6:

6. Defendant Cisco is a California Corporation that maintains regular and established places of business throughout Texas, for example, at its campuses at 12515-3 Research Park Loop, Austin, TX 78759 and at 18615 Tuscany Stone, San Antonio, TX 78258. Cisco is registered to conduct business in the state of Texas and has appointed the Prentice-Hall Corporation Systems, Inc., located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process.

Response: Cisco admits that it conducts business in this judicial district and maintains offices at 12515-3 Research Park Loop, Austin, TX 78759 and at 18615 Tuscany Stone, San Antonio, TX 78258, is registered to conduct business in the state of Texas, and has appointed the Prentice-Hall Corporation Systems, Inc., located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process. Cisco is now a Delaware corporation. Cisco does not contest the exercise of personal jurisdiction or propriety of venue under 28 U.S.C. § 1400(b) as to the '892 patent, but denies that venue in this district is proper as to the '705 patent and denies that venue in this judicial district is convenient or in the interests of justice. Except as expressly admitted, Cisco denies the allegations in paragraph 6 of the Complaint.

Complaint Paragraph 7:

7. By registering to conduct business in Texas and by maintaining facilities in Austin and San Antonio, Cisco has a permanent and continuous presence in the state of Texas and regular and established places of business in the Western District of Texas.

Response: Cisco admits that it conducts business in this judicial district and maintains offices at 12515-3 Research Park Loop, Austin, TX 78759 and at 18615 Tuscany Stone, San Antonio, TX 78258, and is registered to conduct business in the state of Texas. Cisco does not contest the exercise of personal jurisdiction or propriety of venue under 28 U.S.C. § 1400(b) as to the '892 patent, but denies that venue in this district is proper as to the '705 patent and denies that venue in this judicial district is convenient or in the interests of justice. Except as expressly admitted, Cisco denies the allegations in paragraph 7 of the Complaint.

JURISDICTION AND VENUE

Complaint Paragraph 8:

8. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

Response: Cisco admits that this is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq., but denies that it has committed any act of infringement and denies the legal sufficiency of K.Mizra's Complaint.

Complaint Paragraph 9:

9. This Court has original subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

Response: Admitted.

Complaint Paragraph 10:

10. This Court has personal jurisdiction over Cisco because, inter alia, Cisco has a continuous presence in, and systematic contact with, this District and has registered to conduct business in the state of Texas.

Response: Except as expressly admitted in response to paragraph 6 of the Complaint, Cisco denies the allegations in paragraph 10 of the Complaint. Cisco does not contest the exercise of personal jurisdiction or propriety of venue under 28 U.S.C. § 1400(b) as to the '892 patent, but denies that venue in this district is proper as to the '705 patent and denies that venue in this judicial district is convenient or in the interests of justice.

Complaint Paragraph 11:

11. Cisco has committed and continues to commit acts of infringement of K.Mizra's Patents-in-Suit in violation of the United States Patent Laws, and has made, used, sold, offered for sale, marketed and/or imported infringing products into this District. Cisco's infringement has caused substantial injury to K.Mizra, including within this District.

Response: Denied.

Complaint Paragraph 12:

12. Venue is proper in this District pursuant to 28 U.S.C. §§ 1400 and 1391 because Cisco resides in this judicial district, has committed acts of infringement in this District, and maintains regular and established places of business in this District.

Response: Except as expressly admitted in response to paragraph 6 of the Complaint, Cisco denies the allegations in paragraph 12 of the Complaint. Cisco does not contest the propriety of venue under 28 U.S.C. § 1400(b) as to the '892 patent, but denies that venue in this district is proper as to the '705 patent and denies that venue in this judicial district is convenient or in the

interests of justice as to either patent. Except as expressly admitted, Cisco denies the allegations in paragraph 12 of the Complaint.

THE PATENTS-IN-SUIT

Complaint Paragraph 13:

13. The inventions claimed in the Patents-in-Suit were conceived and developed during the 2000s era of the Internet age by two Silicon Valley veterans, Jim Roskind and Aaron Emigh. Both inventors are highly respected technologists and innovators in the fields of computer security and information systems, each with over thirty years of experience in the high-tech computing industry.

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 13 of the Complaint and therefore denies them.

Complaint Paragraph 14:

14. Mr. Emigh is a well-known computer security expert, as well as a named inventor on over 100 United States patents. As a prolific speaker and technologist in the field of cyber security, he has authored several reports on related topics such as the U.S. Secret Service Electronic Crimes Task Force Report on anti-phishing technology and the U.S. Department of Homeland Security Report on online identity theft countermeasures. Mr. Emigh is also an accomplished Silicon Valley technology entrepreneur and innovator. He has been a founder and chief technology officer of several internet companies such as CommerceFlow (now eBay) and Shopkick, developer of the mobile retail application that pioneered the use of in-store beacons at major retailers. Mr. Emigh is currently a co-founder and chief technology officer of Brilliant, the leading smart home control and lighting company that received numerous innovation awards in the industry.

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 14 of the Complaint and therefore denies them.

Complaint Paragraph 15:

15. Dr. Roskind is a named inventor on over 100 United States patents and holds four degrees from MIT in Computer Science and Electrical Engineering, including a PhD. Dr. Roskind's experience spans various roles at prominent internet companies. In the 1990s, he was a co-founder and Chief Scientist at the InfoSeek Corporation, a popular search engine company in the early days of the Internet. He later went on to hold several different roles at Netscape and AOL such as Security Architect, Chief Scientist, and Chief Technology Officer. As the Security Architect there, Dr. Roskind was instrumental in solving most of the security problems related to the Netscape internet browser. In connection with that work, one of his most notable technical accomplishments was the development of Netscape's Java security model. Dr. Roskind is also credited as the architect responsible for designing QUIC, a general purpose computer networking protocol, during his more recent time at Google. QUIC is best known for its use in more than half of all network connections from the Chrome web browser to Google's servers.

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 15 of the Complaint and therefore denies them.

A. U.S. Patent 8,234,705

Complaint Paragraph 16:

16. The '705 patent is titled "Contagion Isolation and Inoculation" and was issued by the United States Patent Office to inventors James A. Roskind and Aaron R. Emigh on July 31, 2012. The earliest application related to the '705 patent was filed on September 27, 2004. A true and correct copy of the '705 patent is attached as Exhibit A.

Response: Cisco admits that what purports, on its face, to be United States Patent No. 8,234,705 entitled "Contagion isolation and isolation" and issued on July 31, 2012, naming inventors James A. Roskind and Aaron R. Emigh, is attached to the Complaint as Exhibit A. Cisco lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in paragraph 16 of the Complaint and therefore denies them.

Complaint Paragraph 17:

17. K.Mizra is the owner of all right, title and interest in and to the '705 patent with the full and exclusive right to bring suit to enforce the '705 patent.

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 17 of the Complaint and therefore denies them.

Complaint Paragraph 18:

18. The '705 patent is valid and enforceable under the United States Patent Laws.

Response: Denied.

Complaint Paragraph 19:

19. The claims of the '705 patent are directed to technological solutions that address specific challenges grounded in computer network security. The security of computer systems and networks is a tremendous concern for modern enterprises, since a breach of an internal network can have severe repercussions, including major financial losses, data theft, disclosure of sensitive information, network disruptions, and data corruption—any of which could have devastating consequences to a business, at any scale. The inventors of the '705 patent understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions

into the network, the most exploitable vulnerabilities of a computer network are the end-user computers that roam throughout various other public and private network domains and then access the presumably secure network day in and day out.

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 19 of the Complaint and therefore denies them.

Complaint Paragraph 20:

20. For example, the '705 patent explains that "[l]aptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization; and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person." See Exhibit A at 1:14-31.

Response: Cisco admits that paragraph 20 of the Complaint quotes language found in the '705 patent but otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 20 of the Complaint and therefore denies them.

Complaint Paragraph 21:

21. While Information Technology (IT) engineers may have been able to keep on-site systems secure and up to date with the technology available at that time, they still faced challenges with off-site devices such as a worker's personal laptop or mobile device which posed significant security risks that could allow attackers or viruses stealth access into a business's network, bypassing IT security measures. For example, the '705 patent states that "[u]pon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm." See id. at 1:34-38.

Response: Cisco admits that paragraph 21 of the Complaint quotes language found in the '705 patent but otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 21 of the Complaint and therefore denies them.

Complaint Paragraph 22:

22. The invention of the '705 patent closes this loophole by verifying that any device attempting to access a company's network meets the company's standards for network security and will not introduce dangerous computer programs or viruses into the company's network. For example, the '705 patent describes that when "a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is required to be quarantined. If the host is required to be quarantined, the host is provided only limited access to the protected network. In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure soft-

ware and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed." See id. at 3:8-20. The '705 patent further describes that "attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user." Id. at 3:20-23.

Response: Cisco admits that paragraph 22 of the Complaint quotes language found in the '705 patent but otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 22 of the Complaint and therefore denies them.

Complaint Paragraph 23:

23. The '705 patent discloses an improvement in computer functionality related to computer network security. For instance, an infected host computer with malicious code, such as a computer virus, worm, exploits and the like ("malware"), poses a serious threat if the malware spreads to other hosts in a protected network. Id. at 1:14-41. The claims of the '705 patent employ techniques, unknown at the time of the invention, that do more than detect malware per se. The claimed techniques quarantine an infected host to prevent it from spreading malware to other hosts while still permitting limited communications with the network to remedy the malware. As a result, the '705 patent provides a technological solution to a problem rooted in computer technology by improving the way networks are secured. And through the implementation and provision of this technology by network security companies such as Cisco, businesses are able to increase their security of vulnerable elements that access their networks.

Response: Denied.

Complaint Paragraph 24:

24. The claims of the '705 patent address the technological problems not by a mere nominal application of a generic computer to practice the invention, but by carrying out particular

improvements to computerized network security technology in order to overcome problems specifically grounded in the field of computer network security. As the '705 patent explains, determining whether a quarantine is required involves detection by a computing device, router, firewall, or other network component as to the infestation or cleanliness of a computer. Id. at 11:15-28. Moreover, the subsequent steps such as quarantining, limiting network access, remediation, and redirecting network communications are functions fundamentally rooted in computer network technology.

Response: Denied.

Complaint Paragraph 25:

25. The claims of the '705 patent recite subject matter that is not merely the routine or conventional use of computer network security that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of assessing and responding to an external network access request in a way that protects the computer network and systems from malicious or undesired breaches. The '705 patent claims specify how a secure network can assess and respond to an external network access request without jeopardizing network integrity.

Response: Denied.

A. U.S. Patent 8,965,892

Complaint Paragraph 26:

26. The '892 patent is titled "Identity-Based Filtering" and was issued by the United States Patent Office to inventor Aaron T. Emigh on February 24, 2015. The earliest application related to the '892 patent was filed on January 4, 2007. A true and correct copy of the '892 patent is attached as Exhibit B.

Response: Cisco admits that what purports, on its face, to be United States Patent No. 8,965,892 entitled "Identity-based filtering" and issued on February 24, 2015, naming inventor Aaron R. Emigh, is attached to the Complaint as Exhibit B. Cisco lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations in paragraph 16 of the Complaint and therefore denies them.

Complaint Paragraph 27:

27. K.Mizra is the owner of all right, title and interest in and to the '892 patent with the full and exclusive right to bring suit to enforce the '892 patent.

Response: Cisco lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 27 of the Complaint and therefore denies them.

Complaint Paragraph 28:

28. The '892 patent is valid and enforceable under the United States Patent Laws.

Response: Denied.

Complaint Paragraph 29:

29. The claims of the '892 patent are directed to technological solutions that address specific challenges rooted in computing technology involving the filtering of electronic content. With the proliferation of electronic documents and content on the internet such as PDFs, webpages, and electronic mail that are accessible via a network address or that traverse a computer network, there is a myriad of undesirable content that a computer user may encounter. See Exhibit B at 1:19-22. The inventors of the '892 patent understood the shortcomings of the traditional approaches to filtering unwanted content that were solely based on including or excluding certain addresses or uniform resource locators (URLs) associated with the document. The '892 patent explains that prior to its invention, "[a] variety of approaches to content filtering have been employed to avoid

undesirable content. Examples of such approaches include blacklisting and whitelisting URLs and sites. However, these approaches fail to discriminate between specific content owners or creators within a site. In some cases, particular participants in a site or service may have more desirable, or less desirable, content than other participants, and present approaches are unable to take advantage of this, leading to either inclusion of objectionable content, or exclusion of desirable content." Id. at 1:23-32.

Response: Cisco admits that paragraph 29 of the Complaint quotes language found in the '892 patent but otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 29 of the Complaint and therefore denies them.

Complaint Paragraph 30:

30. The technological invention of the '892 patent improves upon these conventional techniques for computerized filtering of electronic documents over the internet by extracting and resolving certain data inherent in the electronic document to correlate and determine the reputations of the author or sender of the document and the group in which he or she may be a member of. For example, the '892 patent describes "extracting an identity from a document and/or metadata" and analyzing content with "content analyzing technologies" such as Bayesian filtering or Support Vector Machines. See, e.g., id. at 2:24-36. The '892 patent also discusses further steps of correlating identity, detecting affiliation, and determining reputation associated with electronic documents over a computer network. Id. at 1:37-62. The enhanced filtration techniques taught by the '892 patent can be carried out "programmatically via an API or by retrieving one or more pages from the network and analyzing them." See, e.g., id. at 6:5-67.

Response: Cisco admits that paragraph 30 of the Complaint quotes language found in the '892 patent but otherwise lacks knowledge or information sufficient to form a belief about the truth of the allegations in paragraph 30 of the Complaint and therefore denies them.

Complaint Paragraph 31:

31. The '892 patent claims a way to solve technological problems that existed within the field of electronic documents and computer technology. It provides a technological solution to a problem specific to technology related to electronic documents by improving computer functionality for filtering electronic documents. Faced with the shortcomings of plain filtering techniques such as white-listing or black-listing that existed at the time of the invention, the inventors of the '892 patent developed a far more advanced approach with specific steps for determining and correlating group-related reputation and identity reputation. By utilizing such improvements to electronic content filtering technology, data security companies such as Cisco are able to take advantage of more optimally tailored filtering to block unwanted documents such as electronic mail on computer networks without sacrificing the over-exclusion of desired content.

Response: Denied.

Complaint Paragraph 32:

32. The way in which the claims of the '892 patent address the technological problem is not merely a nominal application of a generic computer to practice the invention. Instead, the claims of the '892 patent implement particular improvements to computerized data filtering technology in order to overcome the problems specifically arising in the field of electronic content filtering.

Response: Denied.

Complaint Paragraph 33:

33. The claims of the '892 patent recite subject matter that is not merely the routine or conventional use of filtering undesired electronic documents that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of determining the reputation associated with electronic documents. The '892 patent claims specify improved computer functionality for extracting certain information and data inherent in the electronic documents for purposes of resolving the reputations associated with the document, author of the document, and groups of which the author may be a member.

Response: Denied.

FIRST CAUSE OF ACTION

(PATENT INFRINGEMENT UNDER 35 U.S.C. §271 OF '705 PATENT)

Complaint Paragraph 34:

34. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

Response: Cisco incorporates its responses to paragraphs 1-33 above.

Complaint Paragraph 35:

35. On information and belief, Cisco has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claims 12 and 19, of the '705 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to Cisco's Identity Services Engine ("ISE"). See, e.g., Exhibit C (https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html, last visited on October 19, 2020).

Response: Denied.

Complaint Paragraph 36:

36. For example, Claim 19 of the '705 patent recites the following:

[preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:

[A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, [B] wherein detecting the insecure condition includes:

[B1] contacting a trusted computing base associated with a trusted platform module within the first host,

[B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,

[C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

[D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

[E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes

[E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,

[E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

[F] permitting the first host to communicate with the remediation host.

Response: Cisco admits the recited claim language is stated in the '705 patent, but denies that Cisco infringes any valid and enforceable claim of the '705 patent.

Complaint Paragraph 37:

37. On information and belief, and based on publicly available information, at least Cisco's ISE satisfies each and every limitation of at least claim 19 of the '705 patent.

Response: Denied.

Complaint Paragraph 38:

38. Regarding the preamble of claim 19, to the extent the preamble is determined to be limiting, Cisco's ISE provides the features described in the preamble. The preamble recites a "computer program product for protecting a network." Cisco's ISE is described below as a critical component for securing the workplace that simplifies the delivery of highly secure network access control.

[IMAGE]

See, e.g., Exhibit C (https://www.cisco.com/c/en/us/products/security/identity-servicesengine/index.html, last visited on October 19, 2020). Thus, to the extent the preamble of claim 19 is limiting, Cisco's ISE meets it.

Response: Cisco admits that paragraph 38 quotes some of the language of claim 19 of the '705 patent and of what appears to be a Cisco document attached as Exhibit C, but otherwise denies the allegations in paragraph 38.

Complaint Paragraph 39:

39. The Cisco ISE also meets all the requirements of limitation A of claim 19. Limitation A requires "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." According to Cisco's ISE datasheet shown below, ISE performs a posture assessment to check whether a device is compliant with the network's security policy—i.e., to detect whether there is an insecure condition on the device.

[IMAGE]

See, e.g., Exhibit D (https://www.cisco.com/c/dam/en/us/products/collateral/security/networkvisibility-segmentation/ise-device-compliance-aag_pdf, last visited on October 22, 2020). For example, Cisco describes that it is critical to determine whether a device has insecure conditions such as outdated software and vulnerabilities that can be exploited by hackers. As the inventors of the '705 patent had first recognized, Cisco also states that "people can unwittingly turn their devices into a real menace on your network."

[IMAGE]

See id. Therefore, Cisco's ISE meets limitation A of claim 19.

Response: Cisco admits that paragraph 39 quotes some of the language of claim 19 of the '705 patent and has quoted and reproduced images from what appears to be a Cisco document attached as Exhibit D, but otherwise denies the allegations in paragraph 39.

Complaint Paragraph 40:

40. The Cisco ISE also meets all the requirements of limitation B1 of claim 19. Limitation B 1 requires that "detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." As mentioned above in Cisco's website, as well as described below in Cisco's ISE Administrator Guide, ISE uses a trusted posture agent such as Cisco AnyConnect that enables the detection of an insecure condition.

[IMAGE]

See Exhibit E at 921. As such, the Cisco ISE meets limitation B1 of claim 19.

Response: Cisco admits that paragraph 40 quotes some of the language of claim 19 of the '705 patent and has reproduced an image from what appears to be a Cisco document attached as Exhibit E, but otherwise denies the allegations in paragraph 40.

Complaint Paragraph 41:

41. The Cisco ISE also meets all the requirements of limitation B2 of claim 19. Limitation B2 requires that "detecting the insecure condition includes" "receiving a response and determining whether the response includes a valid digitally signed attestation of cleanliness." The examples below show that the Cisco ISE meets this limitation of claim 19 of the '705 patent.

[IMAGE]

[IMAGE]

See, e.g., Exhibit F (https://www.cisco.com/c/dam/global/cs_cz/assets/expo2012/pdf/T_SECA4_ISE_Posture_Gorgy_Acs.pdf, last visited on October 22, 2020).

Response: Cisco admits that paragraph 41 quotes some of the language of claim 19 of the '705 patent and has reproduced images from what appears to be a Cisco document attached as Exhibit F, but otherwise denies the allegations in paragraph 41.

Complaint Paragraph 42:

42. The Cisco ISE also meets all the requirements of limitation C of claim 19. Limitation C requires that "the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." As shown above, Cisco's ISE receives responses that confirm whether a device is compliant with the security policy—e.g., the device has the appropriate antivirus software installed. As a further example, the Cisco ISE Datasheet states that the Posture Service checks for the "latest OS patch, antivirus and antispyware packages with current definition file variables," etc.:

[IMAGE]

See, e.g., Exhibit G (https://www.cisco.com/c/en/us/products/collateral/security/identityservices-engine/data sheet_c78-656174.html, last visited on October 22, 2020). Therefore, the Cisco ISE meets limitation C of claim 19.

Response: Cisco admits that paragraph 42 quotes some of the language of claim 19 of the '705 patent and has quoted and reproduced an image from what appears to be a Cisco document attached as Exhibit G, but otherwise denies the allegations in paragraph 42.

Complaint Paragraph 43:

43. The Cisco ISE also meets all the requirements of limitation D of claim 19. Limitation D requires that "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The Cisco

ISE Administrator Guide describes that if ISE detects an insecure condition in the device, it is placed in quarantine under adaptive network control policies whereby network access is denied.

[IMAGE]

Exhibit E at 2.

[IMAGE]

Exhibit E at 208. Therefore, the Cisco ISE meets limitation D of claim 19.

Response: Cisco admits that paragraph 43 quotes some of the language of claim 19 of the '705 patent and has reproduced images from what appears to be a Cisco document attached as Exhibit E, but otherwise denies the allegations in paragraph 43.

Complaint Paragraph 44:

44. The Cisco ISE also meets all the requirements of limitation E1 of claim 19. Limitation E1 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "receiving a service request sent by the first host [and] serving a quarantine notification page to the first host when the service request comprises a web server request." The Cisco ISE Administrator Guide describes that once an insecure or vulnerable device is placed in quarantine, network access is limited with redirection to a different portal such as a quarantine page.

[IMAGE]

See Exhibit E at 1040. Therefore, the Cisco ISE meets limitation E1 of claim 19.

Response: Cisco admits that paragraph 44 quotes some of the language of claim 19 of the '705 patent and has reproduced an image from what appears to be a Cisco document attached as Exhibit E, but otherwise denies the allegations in paragraph 44.

Complaint Paragraph 45:

45. The Cisco ISE also meets all the requirements of limitation E2 of claim 19. Limitation E2 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." As shown in the example below, the ISE may redirect the insecure device to a quarantine notification page and deny access to the network until the insecure condition is remedied.

[IMAGE]

See, e.g., Exhibit F (https://www.cisco.com/c/dam/global/cs_cz/assets/expo2012/pdf/T_SECA4_ISE_Posture_Gorgy_Acs.pdf, last visited on October 22, 2020). The Cisco ISE Administrator Guide also describes remediation options for the insecure device such as allowing it to access a remediation page as shown below. Therefore, the Cisco ISE meets limitation E2 of claim 19.

[IMAGE]

Exhibit E at 974.

Response: Cisco admits that paragraph 45 quotes some of the language of claim 19 of the '705 patent and has reproduced images from what appear to be Cisco documents attached as Exhibits E and F, but otherwise denies the allegations in paragraph 45.

Complaint Paragraph 46:

46. The Cisco ISE also meets all the requirements of limitation F of claim 19. Limitation F requires "permitting the first host to communicate with the remediation host." As discussed

above and also shown below, the Cisco ISE permits the insecure device to communicate with the remediation host. Therefore, the Cisco ISE meets limitation F of claim 19.

[IMAGE]

Exhibit E at 977.

Response: Cisco admits that paragraph 46 quotes some of the language of claim 19 of the '705 patent and has reproduced an image from what appears to be a Cisco document attached as Exhibit E, but otherwise denies the allegations in paragraph 46..

Complaint Paragraph 47:

47. Accordingly, on information and belief, Cisco's ISE meets all the limitations of, and therefore infringes, at least claims 12 and 19 of the '705 patent.

Response: Denied.

Complaint Paragraph 48:

48. As a result of Cisco's infringement of the '705 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Cisco's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Cisco's wrongful conduct.

Response: Denied.

SECOND CAUSE OF ACTION

(PATENT INFRINGEMENT UNDER 35 U.S.C. §271 OF '892 PATENT)

Complaint Paragraph 49:

49. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

Response: Cisco incorporates its responses to paragraphs 1-48 above.

Complaint Paragraph 50:

50. On information and belief, Cisco has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claims 14 and 15, of the '892 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products, including but not limited to those, relating to Cisco's Email Security and Syslog features and functionalities. See, e.g., Exhibit H (https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html, last visited on October 19, 2020).

Response: Denied.

Complaint Paragraph 51:

51. On information and belief, Cisco has been and currently is infringing the '892 patent by the manufacture, use, sale, offer to sell and/or importation of its products, including at least Cisco's Email Security products under 35 U.S.C. § 271.

Response: Denied.

Complaint Paragraph 52:

52. For example, Claim 15 of the '892 patent recites the following:

[preamble] A non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

[A] determining an identity relating to a person, wherein the identity is associated with the electronic document;

[B]determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation;

[C] determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation; and

[D] determining a document reputation, wherein determining the document reputation uses the identity reputation.

Response: Cisco admits the recited claim language is stated in the '892 patent, but denies that Cisco infringes any valid and enforceable claim of the '892 patent.

Complaint Paragraph 53:

53. On information and belief, and based on publicly available information, at least Cisco's Email Security products satisfy each and every limitation of at least claim 15 of the '892 patent.

Response: Denied.

Complaint Paragraph 54:

54. Cisco's Email Security products include all the features of the preamble of claim 15 to the extent the preamble features are determined to be limiting. The preamble of claim 15 recites a "non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address." Cisco's Email Security products are described below as capable of filtering electronic documents such as email on the basis of determining reputation associated with the documents. Therefore, all of the features recited in the preamble are met by Cisco's Email Security products.

[IMAGE]

Id.

Response: Cisco admits that paragraph 54 quotes some of the language of claim 15 of the '892 patent and has reproduced an image from what appears to be a Cisco document attached as Exhibit H, but otherwise denies the allegations in paragraph 54.

Complaint Paragraph 55:

55. Limitation A of claim 15 requires "determining an identity relating to a person, wherein the identity is associated with the electronic document." According to the Cisco document authored by Cisco engineers and shown below, the Cisco products implementing its Syslog software features determine the identities of email senders.

[IMAGE]

See Exhibit I (https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog /syslogsl.pdf, last visited on October 22, 2020).

Also, as a further example, according to the Cisco document authored by Cisco engineers and shown below, the Cisco Email Security products determine the identities of email senders in order to differentiate legitimate senders from sources of email spam.

[IMAGE]

See Exhibit J (https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118380-technote-esa-00.html, last visited on October 19, 2020). Therefore, the Cisco Email Security products meet all the requirements of limitation A of claim 15 of the '892 patent.

Response: Cisco admits that paragraph 55 quotes some of the language of claim 15 of the '892 patent and has reproduced images from what appear to be Cisco documents attached as Exhibits I and J, but otherwise denies the allegations in paragraph 55.

Complaint Paragraph 56:

56. Limitation B of claim 15 requires "determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation." As shown below, Cisco's User Guide for its Email Security Appliance and other similar software products determine an email sender's group or domain and associated reputation of the group. As a result, the Cisco Email Security products practice the requirements of limitation B of claim 15 of the '892 patent.

[IMAGE]

Exhibit K at 313.

Response: Cisco admits that paragraph 56 quotes some of the language of claim 15 of the '892 patent and has reproduced an image from what appears to be a Cisco document attached as Exhibit K, but otherwise denies the allegations in paragraph 56.

Complaint Paragraph 57:

57. Limitation C of claim 15 requires "determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation." As discussed above, Cisco Email Security products determine a reputation of the email sender's identity, which is based in part on the reputation of the group or domain associated with the sender. As a result, the Cisco Email Security products practice limitation C of claim 15 of the '892 patent.

Response: Cisco admits that paragraph 57 quotes some of the language of claim 15 of the '892 patent but otherwise denies the allegations in paragraph 57.

Complaint Paragraph 58:

58. Limitation D of claim 15 requires "determining a document reputation, wherein determining the document reputation uses the identity reputation." As discussed above, Cisco Email Security products determine a reputation verdict for email messages based on the identity reputation. For example, Cisco's User Guide for its Email Security Appliance and other similar software products provide a reputation verdict for email messages using a sender's identity reputation.

[IMAGE]

Exhibit K at 314-15. Therefore, the Cisco Email Security products practice limitation D of the '892 patent.

Response: Cisco admits that paragraph 58 quotes some of the language of claim 15 of the '892 patent and has reproduced an image from what appears to be a Cisco document attached as Exhibit K, but otherwise denies the allegations in paragraph 58.

Complaint Paragraph 59:

59. Accordingly, on information and belief, Cisco's Email Security products meet all the limitations of, and therefore infringes, at least claims 14 and 15 of the '892 patent.

Response: Denied.

Complaint Paragraph 60:

60. As a result of Cisco's infringement of the '892 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Cisco's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Cisco's wrongful conduct.

Response: Denied.

Complaint Prayer For Relief:

WHEREFORE, K.Mizra respectfully requests judgment against Cisco as follows:

A. That the Court enter judgment for K.Mizra on all causes of action asserted in this Complaint;

B. That the Court enter judgment in favor of K.Mizra and against Cisco for monetary damages to compensate it for Cisco's infringement of the Patents-in-Suit pursuant to 35 U.S.C. § 284, including costs and prejudgment interest as allowed by law;

C. That the Court enter judgment in favor of K.Mizra and against Cisco for accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court's entry of final judgment;

D. That the Court enter judgment that this case is exceptional under 35 U.S.C. § 285 and enter an award to K.Mizra of its costs and attorneys' fees; and

E. That the Court award K.Mizra all further relief as the Court deems just and proper.

Response: Cisco denies any liability to K.Mizra, denies that K.Mizra is entitled to any relief from Cisco, and denies all of the allegations contained in K.Mizra's Prayer for Relief. To the extent that any allegations in the Complaint have not been specifically admitted or denied, Cisco denies them.

AFFIRMATIVE DEFENSES

First Affirmative Defense
(Failure to State a Claim)

The Complaint fails to state a claim upon which relief can be granted.

Second Affirmative Defense
(Lack of Standing)

K.Mizra lacks clear title and standing to sue for infringement as the rightful owner of the Patents-in-Suit.

Third Affirmative Defense
(Non-Infringement)

Cisco has not infringed, and does not infringe, under any theory of infringement, any valid, enforceable claim of any of the Patents-in-Suit, whether directly, indirectly, contributorily, through the doctrine of equivalents, or otherwise, and is not inducing and has not induced others to infringe any of the Patents-in-Suit. To the extent K.Mizra alleges indirect infringement, Cisco is not and has not knowingly caused indirect infringement by any third party of any valid and enforceable claim of the Patents-in-Suit, and the accused products have substantial non-infringing uses.

Third Affirmative Defense
(Invalidity)

Each asserted claim of the Patents-in-Suit is invalid for failure to comply with one or more of the statutory requirements specified in Title 35 of the United States Code, including, but not limited to 35 U.S.C. §§ 101, 102, 103, 112, 116, 119, and/or 120.

Fourth Affirmative Defense
(Failure to Mark)

On information and belief, K.Mizra's claims for recovery are barred or limited, in whole or in part, prior to the date on which Cisco received actual notice of K.Mizra's allegations in infringement concerning the Patents-in-Suit, including under 35 U.S.C. § 287.

Fifth Affirmative Defense
(Failure to Disclaim)

On information and belief, K.Mizra's claims for recovery are barred or limited, in whole or in part, by 35 U.S.C. § 288 (failure to disclaim invalid claim(s)).

Sixth Affirmative Defense
(Prosecution Admissions & Estoppel)

K.Mizra's claims are barred, in whole or in part, based upon prosecution history estoppel, prosecution history disclaimer, and/or the internally inconsistent litigation positions K.Mizra or its

predecessors have explicitly or implicitly taken with respect to the Patents-in-Suit in proceedings before the USPTO in the prosecution of one of more of the Patents-in-Suit. As a result, K.Mizra is estopped to maintain that the claims of the Patents-in-Suit are of such scope or have effect against any apparatus made, used or sold by Cisco.

Seventh Affirmative Defense
(Equitable Doctrines)

K.Mizra's claims and relief sought in its Complaint are barred, in whole or in part, by equitable doctrines including estoppel and/or unclean hands based on its past actions and omissions, which are contrary to the claims and relief it now seeks.

Eighth Affirmative Defense
(Limitation on Damages)

K.Mizra's claims for monetary damages are limited by the statute of limitations and, pursuant to 35 U.S.C. § 286, K.Mizra is not entitled to any purported damages suffered more than six (6) years prior to the filing of the Complaint.

Ninth Affirmative Defense
(Breach of Contract)

K.Mizra asserts its claims for infringement of the '705 patent against Cisco in violation of a confidential settlement and license agreement between K.Mizra's predecessors-in-interest and a third party, which K.Mizra produced in discovery on or about September 24, 2021. By suing Cisco in this judicial district and asserting and/or maintaining the claims of infringement set forth in K.Mizra's final infringement contentions against Cisco in this judicial district, K.Mizra materially breached this agreement.

Tenth Affirmative Defense
(License)

Cisco's alleged infringement of the '705 patent is licensed pursuant to the confidential settlement and license agreement entered into by K.Mizra's predecessors-in-interest. By suing

Cisco and/or maintaining the claims of infringement set forth in K.Mizra's final infringement contentions against Cisco in this judicial district, K.Mizra materially breached this license.

Reservation of Rights & Prayer for Relief

Cisco expressly reserves the right to assert any other legal or equitable defenses to which it is shown to be entitled, including all affirmative defenses under Rule 8(c) of the Federal Rules of Civil Procedure, the Patent Laws of the United States, and any other defenses that may now exist or in the future be available based on discovery or further factual investigation in this case.

CISCO'S COUNTERCLAIMS

Defendant and Counterclaim-Plaintiff Cisco Systems, Inc. ("Cisco"), for its counterclaims against Plaintiff and Counterclaim-Defendant K.Mizra, LLC ("K.Mizra"), states as follows:

1. Cisco is a Delaware corporation that K.Mizra has sued for alleged patent infringement in this judicial district.

2. On information and belief, K.Mizra is a Delaware corporation with its principal place of business at 2160 Century Park East #707, Los Angeles, CA 90067.

3. This Court has personal jurisdiction over K.Mizra, which has consented to the exercise of such jurisdiction by filing its original complaint against Cisco.

4. This Court has subject matter jurisdiction over these counterclaims because they arise under the Federal Declaratory Judgements Act, Title 28 U.S.C. §§ 2201 and 2202, and the laws of the United States relating to patents, Title 28 U.S.C. § 1338(a).

5. By filing its claims for patent infringement against Cisco in this Court, K.Mizra has waived the opportunity to contest the propriety of venue over these counterclaims.

6. In its complaint, K.Mizra accused Cisco of infringement of one of more claims of U.S. Patent No. 8,234,705 (the " '705 patent") and of one or more claims of U.S. Patent No. 8,965,892 (the " '892 patent") (collectively, "the Patents-in-Suit").

7. On or about September 24, 2021, K.Mizra produced in discovery a confidential settlement and license agreement between its predecessors-in-interest and a third party ("the Agreement").

8. Cisco is a third party beneficiary to the Agreement.

9. The Agreement precludes K.Mizra's allegations of infringement on the '705 patent.

10. In the alternative, the Agreement at minimum requires K.Mizra to pursue its allegations of infringement against Cisco relating to the '705 patent in the different venue specified in the Agreement.

11. Consequently, an immediate, real, and justiciable controversy exists between Cisco and K.Mizra as to whether K.Mizra is in breach of the Agreement and whether Cisco is licensed.

Count I: Declaration of Breach of Contract

12. Cisco realleges and incorporates by reference the allegations of paragraphs 1 through 11 of its counterclaims.

13. K.Mizra and/or its predecessors-in-interest entered into a valid and binding settlement and license agreement with a third party that precludes its allegations of infringement on the '705 patent. Cisco is a third-party beneficiary of the Agreement.

14. By bringing this suit accusing Cisco of infringing the '705 patent, K.Mizra has breached the releases, licenses, and covenants not to sue in the Agreement.

15. In the alternative, by bringing this suit accusing Cisco of infringing the '705 patent when it did and in this judicial district, K.Mizra has breached the releases, licenses, and covenants not to sue in the Agreement.

16. Absent a declaration of breach of contract, K.Mizra will continue to wrongfully assert the '705 patent against Cisco, thereby continuing to cause Cisco irreparable injury and dam-

age. A judicial declaration is also reasonably calculated to prevent needless litigation in this jurisdiction and other forums, and is necessary to resolve the actual controversy that exists between Cisco and K.Mizra.

17. Cisco thus seeks a judgement declaring that K.Mizra is in breach of the Agreement.

Count II: Declaration of License

18. Cisco realleges and incorporates by reference all allegations of paragraphs 1 through 17 of its counterclaims.

19. K.Mizra and/or its predecessors-in-interest entered into a valid and binding settlement and license agreement with a third party, granting a license to the '705 patent. Cisco is a third-party beneficiary of the Agreement.

20. Absent a declaration that Cisco's alleged infringement is licensed, K.Mizra will continue to wrongfully assert infringement of the '705 patent against Cisco, thereby continuing to cause Cisco irreparable injury and damage. A judicial declaration is also reasonably calculated to prevent needless litigation in this jurisdiction and other forums, and is necessary to resolve the actual controversy that exists between Cisco and K.Mizra.

21. Cisco thus seeks a judgement declaring that Cisco's alleged infringement is licensed under the Agreement and that K.Mizra is accordingly barred from bringing suit alleging that Cisco infringes the '705 patent.

PRAYER FOR RELIEF

WHEREFORE, Cisco respectfully prays for the following relief:

a. A judgement against K.Mizra declaring that K.Mizra has breached the Agreement by bringing this lawsuit alleging infringement of the '705 patent;

b. A judgement against K.Mizra declaring that Cisco's alleged infringement of the '705 patent is licensed pursuant to the Agreement and that K.Mizra is accordingly barred from bringing this suit;

c. A judgment dismissing K.Mizra's Complaint with prejudice;

d. A judgment that this case is exceptional under 35 U.S.C. § 285;

e. A judgment awarding Cisco its costs and attorneys' fees; and

f. A judgment awarding Cisco such other relief as the Court deems just, equitable, and proper.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Cisco respectfully requests a trial by jury on all issues so triable.

Respectfully submitted,

Dated: November 18, 2021

CISCO SYSTEMS, INC.

/s/ Melissa Smith
Melissa Smith

Melissa Smith (State Bar No. 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: 903.934.8450
Facsimile: 903.934.9257

Elizabeth R. Brannen
elizabeth.brannen@strismaher.com
Kenneth J. Halpern
ken.halpern@strismaher.com
STRIS & MAHER, LLP
725 South Figueroa Street, Suite 1830
Los Angeles, CA 90017
Telephone: 213.995.6800
Facsimile: 213.261.0299

Counsel for Defendant Cisco Systems, Inc.

CERTIFICATE OF SERVICE

I certify that, on November 18, 2021, I electronically filed the foregoing pleading with the Clerk of the Court using the CM/ECF System, which will then send a notification of such filing (NEF) to counsel of record for Plaintiff K.Mizra, LLC.

/s/ Melissa R. Smith